Orientações para o treinamento de colaboradores em cibersegurança

ANBIMA

Sumário

Introdução

A cibersegurança é um tema cada vez mais relevante e estratégico para as instituições atuantes nos mercados financeiro e de capitais, que lidam com dados sensíveis e operações críticas para a estabilidade e o desenvolvimento do sistema financeiro nacional. Nesse contexto, os colaboradores dessas organizações desempenham um papel fundamental na prevenção e resposta a ameaças e incidentes cibernéticos, que podem afetar a reputação, a confiança, a continuidade e a conformidade dos negócios.

Como demonstram diversos estudos e levantamentos[1], o fator humano possui ainda grande influência na ocorrência de incidentes cibernéticos. Por isso, é essencial que as organizações invistam na conscientização, no engajamento e na capacitação de seus colaboradores para redução dos riscos e melhoria da segurança da informação e cibernética em todos os níveis e áreas da organização.

Nesse sentido, apresentamos abaixo algumas orientações para auxiliar as organizações na implementação de treinamentos de colaboradores em cibersegurança. Confira também os demais materiais ANBIMA que tratam do tema, disponíveis em: http://anbi.ma/espacociber

Boa leitura!

1. Objetivos dos treinamentos

São objetivos gerais dos treinamentos para colaboradores em cibersegurança:

Devem ser considerados também os seguintes objetivos específicos não exaustivos:

[1] Verizon: *2024 Data Breach Investigations Report*: https://www.verizon.com/business/resources/reports/dbir/. Acessado em: 14/06/2024.

PROMOVER CONSCIENTIZAÇÃO E DISSEMINAR CONHECIMENTOS

- Garantir que todos os colaboradores tenham acesso a princípios de governança, políticas, regras e procedimentos e boas práticas adotados pela organização em segurança cibernética;
- Disponibilizar para acesso de todos os colaboradores da organização e manter atualizados, materiais e recursos, bem como oferecer experiências, que contribuam para o aumento do nível de conhecimento e de conscientização sobre os principais conceitos em cibersegurança, tipos de ameaças cibernéticas e técnicas utilizadas para promover ataques;
- Garantir que todos os colaboradores da organização conheçam os procedimentos para reportar ameaças potenciais ou situações suspeitas;
- Garantir que todos os colaboradores tenham conhecimento de eventuais particularidades relacionadas a função que desempenham e ao exercício de suas responsabilidades na organização no que tange a riscos específicos em segurança cibernética, bem como de ações que devem ser adotadas para mitigá-los.

DESENVOLVER COMPETÊNCIAS E HABILIDADES

- Desenvolver as competências e habilidades de todos os colaboradores da organização para identificar e reportar ameaças cibernéticas ou situações suspeitas e para classificar as informações;
- Garantir o contínuo aprimoramento da equipe responsável pela segurança cibernética e da informação para monitorar riscos e ameaças e para responder a incidentes cibernéticos.

ESTIMULAR O ENGAJAMENTO E A MUDANÇA DE COMPORTAMENTO

- Garantir que todos os colaboradores tenham acesso e assinem termos de ciência e/ou aceite associados a políticas, regras e procedimentos adotados pela organização relacionados à segurança cibernética e da informação;
- Promover uma cultura de segurança cibernética e da informação que estimule a adoção pelos colaboradores de comportamentos e atitudes éticos e que contribuam para prevenir incidentes cibernéticos;
- Estimular os colaboradores para que todos estejam engajados em incorporar as boas práticas no seu dia a dia e a contribuir para a melhoria contínua dos processos e dos controles de segurança da organização.

CONTRIBUIR COM A REDUÇÃO DE RISCOS E A MELHORA DA SEGURANÇA

- Promover exercícios de verificação de assimilação do conhecimento sobre os principais conceitos em cibersegurança, tipos de ameaças cibernéticas e técnicas utilizadas para promover ataques;
- Avaliar e monitorar a eficácia e o impacto dos treinamentos na redução dos riscos e na melhoria do desempenho em segurança cibernética da organização.

2. Metodologia dos treinamentos

A metodologia a ser adotada para os treinamentos de colaboradores em cibersegurança deve buscar favorecer uma aprendizagem significativa, ativa e participativa, que estimule o interesse, a motivação e o engajamento dos colaboradores, que proporcione a troca de experiências, o feedback e a avaliação, e que aplique os conceitos e as boas práticas à realidade e ao contexto da organização.

Nesse sentido, diferentes formatos podem ser adotados de acordo com os objetivos específicos dos treinamentos, o público-alvo, o conteúdo, o tempo e os recursos disponíveis. É recomendável que estes diferentes formatos sejam empregados de acordo com um planejamento prévio que considere um encadeamento das iniciativas visando atingir os objetivos gerais e específicos dos treinamentos.

São exemplos não exaustivos de formatos que podem ser empregados:

- **Estratégias didáticas:** aulas presenciais ou online, com exposição teórica, exemplos práticos, exercícios, simulações, jogos, debates, perguntas e respostas;
- **Materiais de comunicação e de divulgação:** vídeos, podcasts, webinars, e-books, infográficos, cartilhas, newsletters, entre outros;
- **Instrumentos de verificação e de mensuração do nível de conhecimento e de conscientização dos colaboradores:** testes, quizzes, enquetes, pesquisas, avaliações;
- **Ações de sensibilização e de mobilização dos colaboradores:** campanhas, eventos, palestras, workshops, oficinas, hackathons;
- **Ações para incentivar e reconhecer o envolvimento e o desempenho dos colaboradores nos treinamentos:** programas de gamificação, que utilizam elementos de jogos, como pontos, medalhas, rankings, desafios, recompensas;
- **Apoio ou acompanhamento individualizado ou em grupo para os colaboradores:** grupos de discussão que considerem a participação de profissionais experientes ou especializados em segurança cibernética, programas de mentoring, coaching ou tutoria, canal de comunicação para auxílio em questões específicas entre o time responsável pela segurança cibernética na organização e os demais times.

3. Planejamento e execução dos treinamentos

Os treinamentos de colaboradores em cibersegurança devem ser planejados e executados de forma estruturada, sistemática e alinhada à estratégia, às políticas e regras e ao plano para segurança cibernética da organização. Devem abranger todos os colaboradores da organização, independentemente das posições que ocupem, da sua área de atuação, do seu tipo de contrato ou do seu local de trabalho e considerar as especificidades e as necessidades de cada público-alvo, de acordo com o seu perfil, o seu grau de exposição a riscos e as suas expectativas de aprendizagem.

Para isso, recomenda-se considerar as seguintes etapas:

Definição dos objetivos, do escopo, do público-alvo, do conteúdo, da metodologia, do formato, do cronograma, do orçamento e dos indicadores dos treinamentos;

Seleção dos instrutores, dos facilitadores, dos mentores, dos tutores ou dos parceiros externos que irão conduzir ou apoiar os treinamentos;

Desenvolvimento ou aquisição dos materiais, dos recursos, das ferramentas, das plataformas ou dos sistemas necessários para a realização dos treinamentos;

Divulgação e convocação dos colaboradores para os treinamentos, por meio de canais de comunicação interna, como e-mail, intranet, mural, entre outros;

Realização dos treinamentos, seguindo o planejamento estabelecido e monitorando a participação, a interação, a satisfação e o aprendizado dos colaboradores;

Avaliação dos treinamentos, por meio de métodos quantitativos e qualitativos, que permitam medir o impacto, a eficácia, a eficiência e a qualidade dos treinamentos, bem como identificar o que deve mantido, aprofundado e oportunidades de aprimoramento;

Revisão e melhoria dos treinamentos, com base nos resultados da avaliação, nas mudanças no cenário de segurança cibernética, nas novas demandas ou necessidades da organização ou dos colaboradores, na implementação de novas tecnologias e nas regulações e boas práticas de mercado.

4. Conteúdo aplicável aos treinamentos

Quando se fala em cibersegurança, há uma infinidade de conceitos, siglas e termos técnicos que são abordados, o que pode prejudicar o engajamento dos colaboradores nos treinamentos, que são fundamentais para garantir a segurança das organizações. Nesse sentido, estão dispostos abaixo alguns exemplos, não exaustivos, do que poderia ser explorado como conteúdo de treinamentos no sentido de promover maior familiarização com o tema, além de ser base para a capacitação na identificação de potenciais ameaças e na avaliação dos riscos e para a incorporação de boas práticas na rotina.

I. Conceitos importantes em Cibersegurança

Um primeiro passo importante é definir o que é segurança cibernética. Conforme definição dada pelo Gabinete de Segurança Institucional (GSI)[2] do Governo Federal, ela consiste em "ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis". Abaixo, constam outros conceitos importantes em cibersegurança que podem ser abordados nos treinamentos:

- **Ambiente cibernético:** Inclui usuários, redes, dispositivos, software, processos de informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes e computadores. (GSI, 2021)
- **Ameaça:** conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização. (GSI,2021)
- **Aplicativos de terceiros:** programas ou softwares desenvolvidos por entidades externas à organização, que podem ser instalados ou acessados nos dispositivos ou sistemas da organização, e que podem apresentar riscos ou benefícios para a segurança cibernética, dependendo da sua origem, da sua finalidade, da sua qualidade e da sua atualização. (GSI, 2021)
- **Arma Cibernética:** Software, hardware e firmware projetado ou aplicado especificamente para causar dano, por meio do domínio cibernético. Estão incluídas nessa categoria: ferramentas para acesso não-autorizado, vírus, worms, trojans, DoS, DDoS, botnets e rootkits. Além disso, atividades como a engenharia social também são consideradas armas cibernéticas. Armas cibernéticas podem ser utilizadas individualmente ou em conjunto para aumentar os efeitos desejados. (GSI, 2021)
- **Arma Cibernética Cinética:** Software, hardware e firmware projetado ou aplicado especificamente para causar danos físicos, direta ou indiretamente, tanto em pessoas como em equipamentos, somente por meio da exploração de vulnerabilidades dos sistemas e processos de informação. (GSI, 2021)
- **Artefato malicioso:** Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou rede de computadores. (GSI, 2021)
- **Ataque:** Ação que constitui uma tentativa deliberada e não autorizada para acessar ou manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível. (GSI, 2021)
- **Atividade Crítica:** Atividade que deve ser executada visando garantir a consecução de produtos e serviços fundamentais do órgão ou entidade, de forma a atingir os objetivos mais importantes e sensíveis ao tempo. (GSI, 2021)
- **Atividade Maliciosa:** Qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema. (GSI, 2021)
- **Autenticação de 2 Fatores (*2 factor authentication*):** Processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas. (GSI, 2021)
- **Autenticação de Multifatores (MFA)**: Utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário

[2] Glossário de Segurança da Informação (2021): https://www.gov.br/gsi/pt-br/ssic/glossario-de-seguranca-da-informacao-1. Acessado em: 14/06/2024.

conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito). (GSI, 2021)

- **Computação em Nuvem:** Modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN). (GSI, 2021)
- **Crime Cibernético:** Ato criminoso ou abusivo contra redes ou sistemas de informações, seja pelo uso de um ou mais computadores, utilizados como ferramentas para cometer o delito ou tendo como objetivo uma rede ou sistema de informações a fim de causar incidente, desastre cibernético ou obter lucro financeiro. (GSI, 2021)
- **Dado em repouso:** Informação armazenada. A proteção dos dados em repouso não deve ser subestimada, pois informações valiosas podem não ser transmitidas por canais de comunicação, mas apenas serem imóveis. (GSI, 2021)
- **Dado pessoal:** Informação relacionada à pessoa natural identificada ou identificável. (GSI, 2021)
- **Dado pessoal sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (GSI, 2021)
- **Dados processados:** Dados submetidos a qualquer operação ou tratamento, por meio de processamento eletrônico ou por meio automatizado, com o emprego de tecnologia da informação. (GSI, 2021)
- **Defesa de redes:** Programas, atividades e o uso de ferramentas necessárias para facilitá-los [...] conduzidos em um computador, rede ou sistema de informação ou comunicação pelo proprietário ou com o consentimento do o proprietário e, conforme apropriado, os usuários com o objetivo principal de proteger (1) esse computador, rede ou sistema; (2) dados armazenados, processados ou em trânsito nesse computador, rede ou sistema; ou (3) infraestrutura física e virtual controlada por esse computador, rede ou sistema. A defesa da rede não envolve nem exige o acesso ou a realização de atividades em computadores, redes ou sistemas de informação ou comunicação sem autorização dos proprietários ou excedendo o acesso autorizado pelos proprietários. (NIST[3], 2015)
- **Documentos classificados:** Documentos que contenham informação classificada em qualquer grau de sigilo. (GSI, 2021)
- **Engenharia social:** Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da segurança da informação, é considerada uma prática de má-fé para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de indivíduos, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. (GSI, 2021)
- **HTTPS (*hypertext transfer protocol secure*):** sigla que pode ser considerada com um dos fatores para verificar se é seguro clicar em um link de site.

[3] *National Institute of Standards and Technology* – NIST (US): Glossary (2015): https://csrc.nist.gov/glossary/term/phishing#:~:text=Definitions%3A,legitimate%20business%20or%20reputable%20person. Acessado em: 14/06/2024.

- **Incidente Cibernético:** Ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são:
  a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados;
  b) tentativa de utilização não-autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados;
  c) mudanças não-autorizadas de firmware, hardware ou software em um ambiente computacional;
  d) ataques de negação de serviço (DoS); e
  e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada. (GSI, 2021)
- **Informação classificada em grau de sigilo:** Informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada. (GSI, 2021)
- **Informação pessoal:** informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem. (GSI, 2021)
- **Informação sigilosa:** informação submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; e aquela abrangida pelas demais hipóteses legais de sigilo. (GSI, 2021)
- **Informação sigilosa protegida por legislação específica:** Informação amparada pelo sigilo bancário, fiscal, comercial, profissional ou segredo de justiça. (GSI, 2021)
- **Infraestrutura crítica:** Instalações, serviços, bens e sistemas, virtuais ou físicos que, se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança. (GSI, 2021)
- **Inteligência Artificial:** tecnologia que permite a criação de sistemas ou dispositivos capazes de simular ou superar a inteligência humana, por meio de processos de aprendizagem, raciocínio, percepção, decisão e ação, e que pode ser aplicada à segurança cibernética, tanto para fins defensivos quanto ofensivos. (GSI, 2021)
- **Número de Identificação Pessoal (PIN):** Número exclusivo, conhecido somente pelo usuário e pelo sistema, para a autenticação do usuário no sistema. PINs comuns são usados em caixas automáticos para realização de transações bancárias e em chips telefônicos. (GSI, 2021)
- **Vulnerabilidade:** Condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha. (GSI, 2021)

II. Boas práticas a serem adotadas pelos colaboradores

Para que os colaboradores incorporarem boas práticas no seu dia a dia, contribuindo para a melhoria contínua do desempenho da organização em segurança cibernética, é fundamental que sejam descritas nas políticas e

regras relacionadas à cibersegurança as ações e processos a serem adotados individual e coletivamente. Abaixo, encontram-se alguns exemplos não exaustivos de boas práticas recomendadas.

- **Avaliação de Riscos:** Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco. (GSI, 2021)
- **Atualizações de software:** Manter os sistemas operacionais e programas atualizados é fundamental para que sejam instaladas as correções e melhorias lançadas pelos desenvolvedores, que contribuem para mitigar riscos e melhorar a segurança. As áreas responsáveis pela segurança cibernética e da informação podem programar os dispositivos da organização para que sejam atualizados de forma automatizada.
- **Classificação das informações:** Realizar a classificação das informações, conforme processo definido nas políticas e regras da organização, e incluir aviso nos materiais produzidos com relação à sua confidencialidade, sensibilidade e classificação de eventuais dados neles contidos.
- **Conexão Wi-Fi:** Evitar manter opção de conexão automática a redes Wi-Fi, que pode ser conveniente, mas apresenta riscos de segurança. Quando seu dispositivo se conecta automaticamente a uma rede Wi-Fi, pode também se conectar a redes não seguras ou mal-intencionadas sem o seu conhecimento. Evite acessar informações sensíveis, bem como utilização de senhas e informações bancárias, em redes Wi-Fi públicas.
- **Cópia de Segurança (*Backup*):** Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada. (GSI, 2021)
- **Descarte seguro de documentos:** procedimentos para descartar ou destruir informações, documentos, mídias e acervos digitais que contenham informações sensíveis ou confidenciais, de forma a impedir a sua recuperação, o seu uso indevido ou a sua divulgação não autorizada.
- **E-mails corporativos:** uso restrito para uso profissional relacionado à organização e não utilização e/ou cadastramento de e-mails corporativos em plataformas de terceiros sem autorização formal prévia.
- **Política de mesa e telas limpas:** Conjunto de regras e de boas práticas para manter o local de trabalho livre de documentos, dispositivos, anotações (por exemplo, em telas, lousas, blocos de nota etc.) ou outros objetos que contenham informações sensíveis ou confidenciais, de forma a evitar o acesso não autorizado, a perda, o roubo ou o vazamento dessas informações. Destacando a importância de cuidados especiais em viagens e trabalho remoto (sobretudo quando realizado em locais públicos).
- **Riscos das redes sociais:** ameaças e vulnerabilidades relacionadas ao uso de redes sociais, como o compartilhamento de informações pessoais ou profissionais, a exposição a conteúdos falsos ou maliciosos, a invasão de privacidade, a usurpação de identidade, entre outros.
- **Segurança em viagens e em trabalho remoto:** medidas de segurança cibernética a serem adotadas antes, durante e depois de viagens nacionais ou internacionais, como a proteção de dispositivos, a verificação de redes, a atualização de softwares, a criptografia de dados, a utilização de VPN, entre outras.
- **Senhas seguras:** critérios e recomendações para a criação, o uso e a gestão de senhas fortes e seguras ou uso de frases senhas (+24 caracteres), que dificultem a adivinhação, o roubo ou a quebra de senha por meios automatizados.

- **Utilização de serviços de nuvem:** benefícios, riscos e boas práticas para o uso de serviços de armazenamento, processamento ou compartilhamento de dados na nuvem, considerando os aspectos de confidencialidade, integridade, disponibilidade, conformidade e responsabilidade.

III. Ameaças cibernéticas

Para promover a capacitação dos colaboradores na identificação de potenciais ameaças e na avaliação dos riscos à segurança cibernética, é fundamental que os colaboradores tenham conhecimentos básicos sobre táticas, técnicas e procedimentos adotados por agentes maliciosos. É importante também que as organizações disponibilizem aos colaboradores materiais que orientem o processo aplicável para reporte de cada tipo de ameaça. Nesse sentido, recomenda-se a consideração do exemplo de formato de material disponível no Anexo I deste documento. Abaixo, constam alguns exemplos de ameaças cibernéticas comuns.

- **Ataque de Força Bruta:** Um método de acessar um dispositivo obstruído tentando múltiplas combinações de senhas numéricas/alfanuméricas. (NIST, 2015)
- **Bot:** Tipo de malware que, além de incluir funcionalidades de worms, dispõe de mecanismos de comunicação com o invasor, os quais permitem que o computador infectado seja controlado remotamente. O processo de infecção e propagação do bot é similar ao do worm, ou seja, o bot é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. (GSI, 2021)
- **Botnet:** Rede formada por diversos computadores zumbis (infectados com bots). Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam, entre outros. (GSI, 2021)
- **Cavalo de Tróia:** Tipo de malware que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário. (GSI, 2021)
- **Clickjacking:** técnica maliciosa em que uma vítima é induzida a clicar em URL, botão ou outro objeto de tela que ela não tenha percebido e nem pretendido clicar. O clickjacking pode ser realizado de muitas maneiras, uma delas seria carregar uma página web, de forma transparente, atrás de outra página visível, de forma que os links e objetos para clicar são apenas fachadas; ou seja, quando o usuário clicar em um link aparentemente óbvio, ele, na verdade, estará selecionando o link de uma página oculta. (GSI, 2021)
- **Deepfake:** Forma de vídeo manipulado, utilizando técnicas de síntese de imagem humana, que criam renderizações artificiais hiper-realistas de um ser humano. Esses vídeos geralmente são criados pela mistura de um vídeo já existente com novas imagens, áudio e vídeo, para criar a ilusão da fala. Esse processo é realizado por meio de redes contraditórias generativas (GAN). (GSI, 2021) Deepfakes podem ser utilizados de forma maliciosa, a fim de persuadir o colaborador de uma organização a oferecer informações que possam contribuir com atividades que comprometam a segurança cibernética. (GSI, 2021)
- **Espionagem Cibernética:** Atividade que consiste em ataques cibernéticos dirigidos contra a confidencialidade de sistemas de tecnologia da informação, com o objetivo de obter dados e informações sensíveis a respeito de planos e atividades de um governo, instituição, empresa ou pessoa física, sendo geralmente lançados e gerenciados por serviços de inteligência estrangeiros ou por empresas concorrentes. (GSI, 2021)

- **Man-in-the-Middle (MitM):** Um ataque onde o adversário se posiciona entre o usuário e o sistema para poder interceptar e alterar os dados que trafegam entre eles. (NIST, 2015)
- **Phishing:** Uma técnica para tentar adquirir dados sensíveis, tais como números de contas bancárias, através de uma solicitação fraudulenta por e-mail ou num website, em que o perpetrador se faz passar por uma empresa legítima ou pessoa respeitável. (NIST, 2015)
- **Ransomware:** Tipo de malware, que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate. Caso o pagamento do resgate não seja realizado, pode-se perder definitivamente o acesso aos dados sequestrados. (GSI, 2021)
- **Keylogger:** Tipo específico de spyware, com a capacidade de capturar e de armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet banking. (GSI, 2021)
- **Malware:** Software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits. (GSI, 2021)
- **Negação de Serviço (DoS):** Bloqueio de acesso devidamente autorizado a um recurso ou a geração de atraso nas operações e funções normais de um sistema, com a resultante perda da disponibilidade aos usuários autorizados. O objetivo do ataque DoS é interromper atividades legítimas de um computador ou de um sistema. Uma forma de provocar o ataque é aproveitando-se de falhas ou de vulnerabilidades presentes na máquina vítima, ou enviar um grande número de mensagens que esgotem algum dos recursos da vítima, como CPU, memória, banda, entre outros. Para isto, é necessária uma única máquina poderosa, com bom processamento e bastante banda disponível, capaz de gerar o número de mensagens suficiente para causar a interrupção do serviço. (GSI, 2021)
- **Negação de Serviço Distribuída (DDoS):** Atividade maliciosa, coordenada e distribuída, em que um conjunto de computadores ou de dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Embora os ataques do tipo DoS sejam, em geral, perigosos para os serviços de Internet, a forma distribuída é ainda mais perigosa, justamente por se tratar de um ataque feito por várias máquinas, que podem estar espalhadas geograficamente e não terem nenhuma relação entre si, exceto o fato de estarem parcial ou totalmente sob controle do atacante. Além disso, mensagens DDoS podem ser difíceis de identificar por conseguirem facilmente se passar por mensagens de tráfego legítimo, pois enquanto é pouco natural que uma mesma máquina envie várias mensagens semelhantes a um servidor em períodos muito curtos de tempo, como no caso do ataque DoS, é perfeitamente natural que várias máquinas enviem mensagens semelhantes de requisição de serviço regularmente a um mesmo servidor, o que disfarça o ataque DDoS. (GSI, 2021)
- **Quishing (ou QR phishing):** É um tipo de ataque de phishing que utiliza códigos QR para recolher informação sensível, ao solicitar que se realize um scan do código QR disponibilizado por email, o qual redireciona as potenciais vítimas para um website malicioso, onde estas são induzidas a

partilhar dados ou a instalar software malicioso ('quishing' é a contração dos termos 'QR' e 'phishing'). (CNCS[4], 2022)

- **Sabotagem Cibernética:** Ataques cibernéticos contra a integridade e disponibilidade de sistemas e de serviços de tecnologia da informação. (GSI, 2021)
- **Screenlogger:** Tipo específico de spyware. Programa similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que omouseé clicado, ou a região que circunda a posição onde omouseé clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet banking. (GSI, 2021)
- **Smishing:** Combinação das palavras SMS e Phishing, tratando-se da tentativa de adquirir informações pessoais, financeiras ou de segurança por texto mensagem. (EUROPOL[5], 2018)
- **Spoofing:** Ato de falsificar a identidade da fonte de uma comunicação ou interação. É possível falsificar endereço IP, ARP, DNS (conhecido com envenenamento do cache de DNS), endereço MAC, site da web, endereço de e-mail, id de chamador, entre outros. (GSI, 2021)
- **Spyware:** Tipo de malware. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware. (GSI, 2021)
- **Terrorismo Cibernético:** Crime cibernético perpetrado por razões políticas, religiosas ou ideológicas, contra qualquer elemento da infraestrutura cibernética com os objetivos de: provocar perturbação severa ou de longa duração na vida pública; causar danos severos à atividade econômica, com a intenção de intimidar a população; forçar as autoridades públicas ou uma organização a executar, tolerar, revogar ou a omitir um ato; ou abalar ou destruir as bases políticas, constitucionais, econômicas ou sociais de um Estado, organização ou empresa. É principalmente realizado por atos de sabotagem cibernética, organizados e gerenciados por indivíduos, grupos político-fundamentalistas, ou serviços de inteligência estrangeiros. (GSI, 2021)
- **Vírus:** Seção oculta e autorreplicante de um software de computador, geralmente utilizando lógica maliciosa, que se propaga pela infecção (inserindo uma cópia sua e tornando-se parte) de outro programa. Não é autoexecutável, ou seja, necessita que o seu programa hospedeiro seja executado para se tornar ativo. (GSI, 2021)
- **Vishing:** Uma forma de ataque de phishing que ocorre em VoIP, sendo que as vítimas não precisam estar utilizando VoIP. O atacante usa sistemas VoIP para efetuar ligações para qualquer número de telefone, sem cobrança de taxas, e, geralmente, falsifica (spoofing) sua identificação de chamada, a fim de levar a vítima a acreditar que está recebendo um telefonema de uma fonte legítima ou confiável (como um banco, uma loja de varejo, entre outros). (GSI, 2021)
- **Worm:** Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos, e não necessita ser explicitamente executado para se

[4] Glossário (2022) – Centro Nacional de Cibersegurança (CNCS – PT): https://www.cncs.gov.pt/pt/glossario/#linhasobservacao. Acessado em: 03/07/2024.

[5] Guia (2018) – *European Union Agency for Law Enforcement Cooperation* (EUROPOL): https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/take-control-of-your-digital-life. Acessado em: 03/07/2024.

propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de programas instalados em computadores. (GSI, 2021)

Conclusão

Os treinamentos de colaboradores em segurança cibernética são uma das principais medidas para fortalecer a segurança da informação e cibernética das instituições dos mercados financeiro e de capitais, que precisam contar com a atuação consciente, competente e responsável de seus colaboradores para proteger os seus dados, os seus sistemas, as suas redes e as suas operações. Por isso, é fundamental que as organizações invistam na conscientização, no engajamento e na capacitação de seus colaboradores para redução dos riscos e melhoria da segurança. As orientações apresentadas neste documento visam contribuir para a implementação de treinamentos de qualidade, efetivos e alinhados às boas práticas nacionais e internacionais de segurança cibernética. Protegendo o ambiente cibernético, protegemos as informações, os negócios, as organizações, os mercados e as pessoas.

Anexo I

Exemplo de formato de material para orientação do processo aplicável para reporte pelos colaboradores de cada tipo de ameaça às equipes responsáveis pela segurança cibernética das organizações.

AMEAÇAS CIBERNÉTICAS		
[NOME DA AMEAÇA CIBERNÉTICA]		
O que é?	***Como identificar?***	***Como reportar?***
[DEFINIÇÃO CONCEITUAL DA AMEAÇA CIBENÉTICA]	[LISTA DE CARACTERÍSTICAS QUE PERMITEM A IDENTIFICAÇÃO DA AMEAÇA]	[PROCESSO RECOMENDADO PARA O REPORTE DA AMEAÇA, CONSIDERANDO SUAS CARACTERÍSTICAS]
EXEMPLO: Phishing		
O que é?	***Como identificar?***	***Como reportar?***
Uma técnica para tentar adquirir dados sensíveis, tais como números de contas bancárias, através de uma solicitação fraudulenta por e-mail ou num website, em que o perpetrador se faz passar por uma empresa legítima ou pessoa respeitável. (NIST, 2015)	✸ *Verificar se o remetente do e-mail é confiável e se corresponde ao domínio oficial da instituição ou empresa que ele diz representar* ✸ *Desconfiar de e-mails que solicitam informações pessoais, senhas, dados bancários ou outros dados sensíveis* ✸ *Não clicar em links, anexos ou botões sem verificar se eles levam a sites seguros e legítimos* ✸ *Observar se o e-mail contém erros de ortografia, gramática, formatação ou lógica* ✸ *Comparar o e-mail com outros que você recebeu da mesma fonte e verificar se há alguma diferença ou inconsistência*	✸ *Relatar a mensagem na plataforma de correio eletrônico utilizada, marcando-a como spam ou phishing* ✸ *Informar a área responsável pela segurança cibernética e da informação da instituição, mas não encaminhando o link sem que isso seja previamente alinhado e/ou solicitado* ✸ *Seguir as orientações e protocolos estabelecidos pela instituição para lidar com esse tipo de situação, como alterar senhas, bloquear contas ou dispositivos, etc.* ✸ *Alertar os colegas e superiores sobre a tentativa de golpe*